

REMARKS/ARGUMENTS

In view of the amendments made to the specification, and in view of the following remarks, reconsideration of the application is respectfully requested.

1. Priority

The Examiner has required that the application contain a specific reference to a prior application in the first sentence of the specification or in an application data sheet in order to receive the benefit of an earlier filing date under 35 U.S.C. § 121. By the present amendment, the specification has been amended to indicate that it is a divisional of U.S. Application Serial No. 07/479,666 filed on February 13, 1990, now U.S. Patent No. 6,507,909. Applicant respectfully submits that the application is now in full compliance with 35 U.S.C. § 121 and thus should receive the benefits of the earlier filing date.

2. Drawings

The Examiner has required formal drawings in reply to this Office Action. Please note that formal drawings are provided herewith.

3. Double Patenting

Claim 28 has been objected to as being an exact duplicate of claim 26. In response, claim 28 has been canceled.

4. Rejection Under 35 U.S.C. § 102

Claims 21-26 and 28 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Atalla (U.S. Patent No. 4,315,101). This rejection is respectfully traversed.

The present invention relates to a method for improving security on a computer system wherein a process identifier is used to indicate to a user when a trusted path has been established. Essentially, the process identifier is associated with each user during the login process. In one embodiment, as covered by claim 22, this process identifier may be a pseudo-randomly generated alpha-numeric tag which is associated with a user throughout his/her computing session. The process identifier feature of the invention is useful if untrusted code can temporarily disable or delay the effect of activation of a secure attention key. For example, sometimes untrusted code can send a reset command to some terminals. While these terminals are resetting, activation of the secure attention key has no effect. Such a technique may allow untrusted code (presumably maliciously written by someone attempting to obtain unauthorized access to the system) to trick the user into thinking a trusted path has been established when, in fact, it has not. The process identifier feature of the invention inhibits such trickery by displaying the process identifier to the user, allowing the user to distinguish between actual and emulated trusted paths.

As shown in Figure 6 of the subject application, when a user initially logs onto the computer system through the secure server (SSVR) 12, a randomly generated process identifier is assigned to the user. This activity is represented by step 310. In one embodiment, this process identifier comprises alphabetic characters. The process identifier is then stored in trusted memory by the SSVR12 and displayed to the user by the SSVR12 at step 320. If the trusted computing base (TCB) determines the trusted path has not been established, the process identifier is not displayed to the user. Each time a trusted path is established between the SSVR12 and the user, the SSVR12 displays the

user process identifier at step 340. By observing the displayed process identifier, the user is assured that an actual trusted path has been established.

By contrast, U.S. Patent No. 4,315,101 is directed to improving security of data transmission between stations. More particularly, the improved security is provided by not requiring transmission of personal identification number data from the originating or user station to the destination or processing station. In the case of, for example, debiting an account or dispensing cash at the end of a transaction, an output 110 is generated upon favorable comparison of two ACK-TRAC signals as described in column 8, lines 6-12.

This patent simply does not disclose or suggest displaying a process identifier to a user, let alone, displaying the process identifier to the user through the trusted path upon the user's subsequent entry into a trusted environment, as required by claim 21. Since these aspects of the invention are entirely missing from the prior art, Applicant respectfully submits that independent claim 21 and dependent claims 22-26 should be allowed.

5. Claim Rejection Under 35 U.S.C. § 103

Claim 27 has been rejected under 35 U.S.C. § 102(b) as being anticipated by or, in the alternative, under 35 U.S.C. § 103(a) as obvious over Atalla (U.S. Patent No. 4,315,101) in view of National Institute of Standards and Technology, "EES modes of operation." This rejection is respectfully traversed.

The present invention is directed to a method for executing trusted commands issued by a user. Claim 27 recites trusted means for receiving a parsed command via a trusted path; means for displaying a representation of the parsed command to a user for verification; and trusted means for executing the verified parsed command. This combination of claim features is supported by disclosure in Applicant's specification that a command requesting information is executed by a trusted computing base (TCB) 10,

the secure server (SSVR) 12 responds by displaying a complete representation of the requested command, as well as the requested information, i.e., a standard human readable representation of the command is displayed. Therefore, if the user's command is improperly parsed, or modified in an unauthorized manner, the user will be able to observe the differences. This inhibits an untrusted subject from fooling the user into believing that he or she is observing the results of the submitted command when, in fact, that command has actually been altered. By parsing the command in untrusted code and verifying the request in a trusted code, the overall complexity of the TCB is decreased. The display of "what is about to be done" may, of course, vary from one command to another.

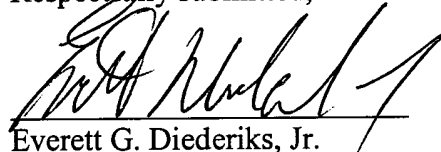
By contrast, the Atalla reference is directed to a method and apparatus for improving the security of data transmission between stations and controlling secure transactions from remote locations in a data transfer system. For example, an authorized individual located at a correspondent office "A", such as a bank or trucking company, is able to control a transaction, such as a wire transfer, from a correspondent office "B" with the aid of circuitry, files and operation of the central office (see column 8, lines 24-44). While the system does indicate an output 110 being generated upon favorable comparison of two ACK-TRAC signals by a comparator 107, for example to indicate the completion of a transaction such as debiting an account or dispensing cash (see column 8, lines 3-12), **the Atalla reference does not disclose or suggest displaying a representation of the parsed command to the user for verification.** For example, if an individual were to command a wire transfer in accordance with the Atalla reference, the Atalla arrangement would not include means to generate a parsed command or means for receiving such a command via a trusted path. In addition, there is no means for displaying a representation of the parsed command to the user for verification. Consequently, Atalla fails to anticipate and does not suggest any modification that would render claim 27 obvious to a person of ordinary skill in the art; Atalla does not render claim 27 unpatentable.

6. Information Disclosure Statement

The Applicant, in the utmost of the good faith and candor with the Patent Office, would like to make the Examiner aware of U.S. Patent Application Serial No. 09/514,978 which represents another divisional application stemming from the same parent application of the present case. The enclosed IDS merely makes of record the art cited in the related case, even though the subject matter claimed is patentably distinct as evidenced by the prior presented restriction requirement.

In view of the above remarks, the amendments to the specification, drawings and the cancellation of claim 28, it is respectfully requested that the claims be allowed and the application pass to issue. If the Examiner should have any questions concerning the allowance of this application, he is cordially invited to contact the undersigned at the number provided below to further expedite the prosecution.

Respectfully submitted,



Everett G. Diederiks, Jr.
Attorney for Applicant
Reg. No. 33,323

Date: April 22, 2004
DIEDERIKS & WHITELAW, PLC
12471 Dillingham Square, #301
Woodbridge, VA 22192
Tel: (703) 583-8300
Fax: (703) 583-8301